UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,351	12/11/2001	Howard G. Pinder	A-7274	8293

5642 7590 07/08/2008

SCIENTIFIC-ATLANTA, INC.
INTELLECTUAL PROPERTY DEPARTMENT
5030 SUGARLOAF PARKWAY
LAWRENCEVILLE, GA 30044

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
07/08/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOmail@sciatl.com

Office Action Summary	Application No.	Applicant(s)	
	10/015,351	PINDER ET AL.	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-124* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-124* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on .

2. Claims 1-124 are pending.

3. Claims 1, 24, 38, 55, 69, 77, 83, 92, 100, 105, 110, 115, and 120 are amended.

4. Applicant's arguments have been fully considered but they are not persuasive.

Response to Arguments

1. Applicants with respect to claims 1, 24, 38, 55, 69, 77, 83, 92, 100, 105, 110, 115, and 120 on pages 37, 41, 45, 55, 53, 57, 61, 65, 69, 73, 77, 81, and 85 of the remarks argue that "In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky's* disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet.* It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so."

Examiner respectfully disagrees and asserts that Rabowsky discloses "A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM (see col. 9, line 65-col. 10, line 6)", which clearly similar to Bartholet, the encryption/decryption key is generated at the receiver location or any location that has an encryptor and/or a decryptor. Therefore, Bartholet does not teach away from Rabowsky. Additionally, in the previous office action Rabowsky and Bartholet have been combined to implement the scheme of multi-layer encryption of the receiving packets taught by Bartholet in the system of Rabowsky, which does not require that the teachings of the two arts have to be the same or about the same type of system. The scheme of multi-layer encryption of data can be implemented in any type of system of data processing, where an encryptor and/or a decryptor are present. Furthermore, the protection of the received content while being stored and reduction of the risk of known-plaintext attack on the received content provide ample motivation for a person of ordinary skill in the art to combine Rabowsky and Bartholet.

2. In light of the above the previous rejections are maintained while considering the amendments to the independent claims as follows:

Claim Rejections - 35 USC § 103

Claims 1-124 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabowsky (6,141,530) in view of Bartholet et al (2002/0114453 A1).

Regarding claims 1, 24, 38, 50, 55, 58, 69, 77, 83, 92, 100, 105, 110, 115 and 120, Rabowsky discloses:

receiving from a headend of the subscriber network a first ciphertext packet at the receiver (see, for example, col. 2, lines 27-46; col. 3, lines 33-35; col. 4, lines 21-32; col. 8, lines 51-62);

an input port adapted to receive a first key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using the first key (see, for example, Fig. 2; col. 4, lines 21-32; col. 8, lines 51-62; col. 10, lines 1-11);

a key generator adapted to generate a key (see, for example, col. 6, lines 52-56; col. 9, line 65-col. 10, line 10);

a storage device in communication with the cryptographic device adapted to store the ciphertext packet and the keys (see, for example, col. 8, lines 51-62; col. 10, lines 12-25); a cryptographic device in communication with the input port and the key generator (see, for example, col. 9, lines 3-11; col. 9, lines 43-45; col. 9, line 65-col. 10, line 10); and

Rabowsky, however, does not expressly disclose a scheme to use cryptographic algorithms to apply further encryption to the incoming encrypted packets from headend

without first converting them to cleartext packets, in order to convert them into ciphertext packets with one or more layers of encryption.

Bartholet, on the other hand, discloses:

applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet (see, for example, [0012], lines 9-22, where at the storage system as one option the received encrypted packets are further encrypted and then stored);

applying to the second ciphertext packet a second cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet (see, for example, and [0022], where multi-layer encryption may be employed).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Regarding claims 2, 15, 93, 94, 106 and 116, Rabowsky in view of Bartholet discloses:

wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of: storing the third ciphertext packet at the subscriber location (see, for example, col. 1, lines 60-67; col. 8, lines 42-67).

Regarding claims 3, 40, and 84, Rabowsky in view of Bartholet discloses:

wherein the third ciphertext packet is stored in a device external to the receiver (see, for example, Fig. 2, storage media 78).

Regarding claims 4, 7, 27, 36, 37, 39 and 85, Rabowsky in view of Bartholet discloses:

wherein the third ciphertext packet is stored in an internal storage device of the receiver (see, for example, col. 10, lines 13-15).

Regarding claims 5, 35, 47 and 59, Bartholet discloses:

wherein the third ciphertext packet corresponds to a cleartext packet that has been encrypted by a 3DES algorithm (see, for example, page 94, Fig. 4.1(b), encryption operation).

Regarding claims 6 and 97, Rabowsky in view of Bartholet discloses:

wherein the first ciphertext packet includes encrypted content of a program distributed by the subscriber network (see, for example, col. 1, lines 467).

Regarding claims 7, 51, 61, 63, 70, 73, 75 and 78, Bartholet discloses:

applying a third cryptographic algorithm to the third ciphertext packet to convert the third ciphertext packet to a cleartext packet (see, for example, page 94, Fig. 4.1(b), decryption operation).

Regarding claims 8, 53, 65, 90, 103, 108, 113, 118 and 123, Rabowsky in view of Bartholet discloses:

converting the cleartext packet from a first format to a second format (see, for example, col. 2, lines 51-62; col. 3, line 9-15).

Regarding claims 9, 54, 66, 91, 104, 109, 114, 119 and 124, Rabowsky in view of Bartholet discloses:

wherein the first format is an MPEG format (see, for example, col. 4, lines 6-10).

Regarding claims 10, 18, 23, 30, 49, 52, 57, 64, 74, 76, 87, 89, 96, 102, 112 and 122, Rabowsky in view of Bartholet discloses:

wherein the third cryptographic algorithm is a 3DES algorithm (see, for example, col. 4, lines 20-32).

Regarding claims 11, 12, 31, 32, 33, 34, 43, 46, 60, 62, 71, 72, 79, 80, 86 and 98, Rabowsky in view of Bartholet discloses:

wherein the first cryptographic algorithm is a DES algorithm (see, for example, col. 4, lines 20-32).

Regarding claims 13 and 25, Bartholet discloses:

wherein the act of converting the first ciphertext packet to the second ciphertext packet removes a layer of encryption from the first ciphertext packet (see, for example, [0010]; [0011]; [0022]).

Regarding claims 14, 19 and 26, Bartholet discloses:

wherein the act of converting the second ciphertext packet to the third ciphertext packet adds a layer of encryption to the second ciphertext packet (see, for example, [0022]).

Regarding claims 15, 94 and 99, Rabowsky in view of Bartholet discloses:

receiving a first key from the headend, wherein the first key is applied to the first ciphertext packet with the first cryptographic algorithm (see, for example, col. 10, lines 7-11).

Regarding claims 16, 28 and 68, Rabowsky in view of Bartholet discloses:

generating an encryption key at the receiver, wherein the encryption key is applied to the second ciphertext packet with the second cryptographic algorithm (see, for example, col. 11, lines 47-53).

Regarding claims 17, 29, 67, 81, 82, 88, 95, 101, 107, 111, 117, and 121, Rabowsky in view of Bartholet discloses:

receiving at least one key associated with the first ciphertext packet; and applying a third cryptographic algorithm with the at least one key and the encrypt key to convert the third ciphertext packet to a cleartext packet (see, for example, Rabowsky, col. 9, line 65-col. 10, line 10; Bartholet, [0028] and [0029]).

Regarding claims 20 and 41, Rabowsky in view of Bartholet discloses:

generating at least one encryption key at the receiver, wherein the at least one encryption key is applied to the first ciphertext packet with the first cryptographic algorithm and the second ciphertext packet with the second cryptographic algorithm (see, for example, Rabowsky, col. 11, lines 47-53; Bartholet, [0010], [0028] and [0029]).

Regarding claims 21, 22, 41, 42, 44, 48 and 56, Rabowsky in view of Bartholet discloses:

wherein the at least one encryption key is a first encryption key and a second encryption key, the first encryption key is applied to the first ciphertext packet with the first cryptographic algorithm, and the second encryption key is applied to the second ciphertext packet with the second cryptographic algorithm (see, for example, Bartholet, [0010], [0022], [0029] and [0035]).

Regarding claim 45, Rabowsky in view of Bartholet discloses:

wherein the cryptographic algorithm includes a first function and a second function, the first application of the cryptographic algorithm includes using the first function, and the second application of the cryptographic algorithm includes using the

second function (see, for example, col. 4, lines 20-30).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Abdulhakim Nobahar/
Examiner, Art Unit 2132

July 01, 2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132